B. Amendments to the Claims

Claim 1 (Previously presented): A method for generating prime numbers for use in encryption, the method comprising the steps of:

a. generating a random number 'n';

b. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

c. declaring the random number 'n' to be composite;

if the random number 'n' is not an exact power of the another positive integer, then:

d. performing an extension ring test on the random number 'n'; and

e. providing the random number 'n' to an encryption system, based on the result of the extension ring test.

Claim 2 (Original): The method as recited in claim 1 wherein the step of performing the extension ring test comprises the steps of:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n) \bmod(f(x), n)$, for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number 'n' to be composite; and

if $[g(x)]^n = g(x^n) \bmod(f(x), n)$, for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number 'n' to be prime.

Claim 3 (Original): The method as recited in claim 1 wherein the step of performing the extension ring test comprises the steps of:

a. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

i. the number 'r' is a prime number;

ii. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r}\log_2 n)$;

iii. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

iv. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

b. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1;

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

i. declaring the number 'n' to be composite;

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

ii. declaring the number 'n' to be prime; and

if a number 'r' satisfying the conditions specified in step a exists, then:

c. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r}\log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

i. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

ii. declaring the random number 'n' to be prime.

Claim 4 (Previously presented): A method for generating prime numbers for use in encryption, the method comprising the steps of:

a. generating a random number 'n';

b. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

c. declaring the random number 'n' to be composite;

if the random number 'n' is not an exact power of the another positive integer, then:

d. performing an extension ring test, the extension ring test comprising:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;
2. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r} \log_2 n)$;
3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and
4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step i exists, then

for all values of the number 'r' less than the random number 'n':

ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

2. declaring the number 'n' to be prime;

if a number 'r' satisfying the conditions specified in step i exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. declaring the random number 'n' to be prime;

and

e. providing the random number 'n' to an encryption system if the random number 'n' is declared to be prime in the extension ring test.

Claim 5 (Canceled)

Claim 6 (Canceled)

Claim 7 (Previously presented): A method for deterministically testing primality of a random number 'n' in polynomial time for use in encryption, the method comprising the steps of:

a. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

b. declaring the random number 'n' to be composite;

if the random number 'n' is not an exact power of the another positive integer, then:

c. performing an extension ring test; and

d. providing the random number 'n' to an encryption system, based on the result of the extension ring test.

Claim 8 (Original): The method as recited in claim 7 wherein the step of performing the extension ring test comprises the steps of:

a. choosing a set of polynomials g(x);

b. choosing a polynomial f(x);

if $[g(x)]^n \neq g(x^n)$ mod(f(x), n), for the chosen f(x) and any g(x) belonging to the chosen set of polynomials g(x) then:

c. declaring the random number 'n' to be composite; and

if $[g(x)]^n = g(x^n)$ mod(f(x), n), for the chosen f(x) and all g(x) belonging to the chosen set of polynomials g(x) then:

d. declaring the random number 'n' to be prime.

Claim 9 (Original): The method as recited in claim 7 wherein the step of performing the extension ring test comprises the steps of:

a. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

i. the number 'r' is a prime number;

ii. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r}\log_2 n)$;

iii. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

iv. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

b. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

i. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

ii. declaring the number 'n' to be prime;

if a number 'r' satisfying the conditions specified in step a exists, then:

c. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r}\log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

i. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

ii. declaring the random number 'n' to be prime.

Claim 10 (Previously presented): A method for deterministically testing primality of a random number 'n' in polynomial time for use in encryption, the method comprising the steps of:

a. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

b. declaring the random number 'n' to be composite; ~~and~~

if the random number 'n' is not an exact power of the another positive integer, then:

c. performing an extension ring test, the extension ring test comprising:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;
2. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r} \log_2 n)$;
3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and
4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step ~~a~~ i exists, then for all values of the number 'r' less than the random number 'n':

ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

2. declaring the number 'n' to be prime; and

if a number 'r' satisfying the conditions specified in step ~~a~~ i exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. declaring the random number 'n' to be prime;

and

d. providing the random number 'n' to an encryption system if the random number 'n' is declared to be prime in the extension ring test.

Claim 11 (Canceled)

Claim 12 (Canceled)

Claim 13 (Currently amended): ~~A system~~ A primality tester for deterministically testing primality of a random number 'n' in polynomial time by performing an extension ring test, for use in encryption, ~~the primality tester performing an extension ring test on the random number 'n' so as to determine whether the random number 'n' is prime, wherein the extension ring test comprises:~~ the primality tester comprising:

a. means for determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

i. the number 'r' is a prime number;

ii. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r} \log_2 n)$;

iii. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

iv. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

b. means for performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

i. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

ii. declaring the number 'n' to be prime;

if a number 'r' satisfying the conditions specified in step a exists, then:

c. means for checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

i. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

ii. declaring the random number 'n' to be prime.

Claim 14 (Canceled)

Claim 15 (Canceled)

Claim 16 (Currently amended): A prime number generator, the prime number generator being connected to an encryption system, the encryption system using prime numbers generated by the prime number generator in encryption, the prime number generator comprising:

a. a random number generator the random number generator generating a random number 'n'; and

b. a primality tester, the primality tester performing an extension ring test on the random number 'n' so as to determine whether the random number 'n' is prime, wherein the primality tester comprises:

i. means for determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

i.i. the number 'r' is a prime number;

i.ii. the largest prime factor 'q' of (r – 1) is greater than or equal to ($4\sqrt{r}\log_2 n$);

i.iii. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

i.iv. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step a exists, then for all values of the number 'r' less than the random number 'n':

ii. means for performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

ii.i. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

ii.ii. declaring the number 'n' to be prime;

if a number 'r' satisfying the conditions specified in step a exists, then:

iii. means for checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to ($2\sqrt{r}\log_2 n$);

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and ($2\sqrt{r}\log_2 n$), then:

iii.i. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

iii.ii. declaring the random number 'n' to be prime.

Claim 17 (Canceled)

Claim 18 (Canceled)

Claim 19 (Canceled)

Claim 20 (Canceled)

Claim 21 (Canceled)

Claim 22 (Previously presented): A computer program product for use with a computer, the computer program product comprising a computer usable medium having a computer readable program code embodied therein for generating prime numbers for use in encryption, the computer readable program code comprising instructions for:

a. generating a random number 'n';

b. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

c. declaring the random number 'n' to be composite;

if the random number 'n' is not an exact power of the another positive integer, then:

d. performing an extension ring test, the extension ring test comprising:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;

2. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r}\log_2 n)$;

3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and

4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step i exists, then for all values of the number 'r' less than the random number 'n':

ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

2. declaring the number 'n' to be prime; and

if a number 'r' satisfying the conditions specified in step i exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r}\log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r}\log_2 n)$, then:

1. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r}\log_2 n)$, then:

2. declaring the random number 'n' to be prime;

and

e. providing the random number 'n' to an encryption system if the random number 'n' is declared to be prime in the extension ring test.

Claim 23 (Previously presented): A computer program product for use with a computer, the computer program product comprising a computer usable medium having a computer readable program code embodied therein for deterministically testing primality of a random number 'n' in polynomial time for use in encryption, the computer readable program code comprising instructions for:

a. checking if the random number 'n' is an exact power of another positive integer;

if the random number 'n' is an exact power of the another positive integer, then:

b. declaring the random number 'n' to be composite;

if the random number 'n' is not an exact power of the another positive integer, then:

c. performing an extension ring test, the extension ring test comprising:

i. determining the smallest number 'r' less than the random number 'n', the number 'r' satisfying the following conditions:

1. the number 'r' is a prime number;
2. the largest prime factor 'q' of $(r - 1)$ is greater than or equal to $(4\sqrt{r}\log_2 n)$;
3. $n^{(r-1)/q} \neq 1 \bmod (r)$; and
4. the greatest common divisor of the number 'r' and the random number 'n' is equal to 1;

if no number 'r' satisfying all the conditions specified in step i exists, then for all values of the number 'r' less than the random number 'n':

ii. performing a check whether the greatest common divisor of the number 'r' and the random number 'n' is greater than 1; and

if the greatest common divisor of 'r' and 'n' is greater than 1 for any value of the number 'r', then:

1. declaring the number 'n' to be composite; and

if the greatest common divisor of 'r' and 'n' is equal to 1 for all values of the number 'r', then:

2. declaring the number 'n' to be prime;

and

if a number 'r' satisfying the conditions specified in step i exists, then:

iii. checking whether $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$;

if $(x + a)^n \neq x^n + a \bmod (n, x^r - 1)$ for any integer value of 'a' between 1 and $(2\sqrt{r} \log_2 n)$, then:

1. declaring the number 'n' to be composite; and

if $(x + a)^n = x^n + a \bmod (n, x^r - 1)$ for all integer values of 'a' from 1 to $(2\sqrt{r} \log_2 n)$, then:

2. declaring the random number 'n' to be prime;

and

d. providing the random number 'n' to an encryption system if the random number 'n' is declared to be prime in the extension ring test.